

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

AUTOSCRIBE CORPORATION

Plaintiff

v.

M&A VENTURES, LLC
Defendant.

§
§
§
§
§
§
§
§
§

Case No. 1:24-cv-04282-SCJ

JURY TRIAL DEMANDED

M&A VENTURES LLC'S OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Background of the '621 Patent	2
III.	Legal Standard	3
IV.	Argument	4
A.	“perform[ing] each software process required to maintain compliance with one or more information security standards”	4
B.	“sensitive financial account information”	7
C.	“obtainin[ing]” and “forward[ing]” a payment amount.....	8
	1. “Payment amount” refers to money paid to the merchant, not just information about the payment.	9
	2. The secure server must “forward” at least a portion of the payment, not merely cause another to do so.	11
D.	“authenticate[s] a payee” / “authenticating the payee”	13
E.	“function”	16
F.	“providing a non-sensitive data token to the merchant...without providing the non-sensitive data token to the payer”	17
G.	“receiving the non-sensitive electronic data token from the secure server, wherein...the secure server does not provide the non-sensitive electronic data token to the payer”	21
H.	“generating a uniform resource locator (url),... the url comprising either: a dynamic url generated by the secure server...; or a static url and a hypertext transport protocol (http) parameter... ”	24
I.	The “representation of the non-sensitive electronic data token” terms	27
	1. Intrinsic and extrinsic evidence indicates that a “representation” differs from the thing it represents.	28
	2. Different intrinsic evidence demonstrates that a “representation of the token” includes the token.	29

3. Any attempt to reconcile the evidence yields a nonsensical claim construction.....	31
V. Conclusion	32

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Becton, Dickinson and Co. v. Tyco Healthcare Group, LP</i> , 616 F.3d 1249 (Fed. Cir. 2010).....	29
<i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018).....	6
<i>Eon Corp. IP Holdings v. Silver Spring Networks</i> , 815 F.3d 1314 (Fed. Cir. 2016).....	18
<i>Every Penny Counts, Inc. v. Am. Express Co.</i> , 563 F.3d 1378 (Fed. Cir. 2009).....	18, 19
<i>HZNP Medicines LLC v. Actavis Labs. UT, Inc.</i> , 940 F.3d 680 (Fed. Cir. 2019).....	28, 31
<i>Interval Licensing LLC v. AOL, Inc.</i> , 766 F.3d 1364 (Fed. Cir. 2014).....	3, 4, 6
<i>Nautilus, Inc. v. Biosig Instruments, Inc.</i> , 572 U.S. 898 (2014).....	3, 4
<i>O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.</i> , 521 F.3d 1351 (Fed. Cir. 2008).....	15, 17
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005).....	3, 12, 16
<i>PPC Broadband, Inc. v. Corning Optical Commc'ns. RF, LLC</i> , 815 F.3d 747 (Fed. Cir. 2016).....	15
<i>Process Control Corp. v. HydReclaim Corp.</i> , 190 F.3d 1350 (Fed. Cir. 1999).....	32
<i>Schindler Elevator Corp. v. Otis Elevator Co.</i> , 593 F.3d 1275 (Fed. Cir. 2010).....	20, 23
<i>Teva Pharms. USA, Inc. v. Sandoz, Inc.</i> , 574 U.S. 318 (2015).....	4
<i>Wasica Fin. GmbH v. Cont'l Auto. Sys., Inc.</i> , 853 F.3d 1272 (Fed. Cir. 2017).....	11

<i>Wi-Fi One, LLC v. Broadcom Corp.</i> , 887 F.3d 1329 (Fed. Cir. 2018).....	12
--	----

<i>Wisconsin Alumni Rsch. Found. v. Apple Inc.</i> , 905 F.3d 1341 (Fed. Cir. 2018).....	14
---	----

Statutes

35 U.S.C. § 112(b)	3
--------------------------	---

I. INTRODUCTION

Four of the terms proposed for construction in this case are indefinite. M&A submits a declaration from Dr. Michael Shamos¹ in support of these indefiniteness arguments. Dr. Shamos has a Ph.D. from Yale University in Computer Science and for twenty years taught one of the few graduate courses on Electronic Payment Systems in the world. Autoscribe has not challenged Dr. Shamos's qualifications or his status as a person of ordinary skill in the art, did not depose Dr. Shamos, and did not submit a competing declaration. Dr. Shamos's testimony on indefiniteness is un rebutted and his conclusions should be adopted.

For several of the remaining terms at issue in this case, M&A submits constructions that embody the plain and ordinary meaning of the terms while Autoscribe merely submits "plain and ordinary meaning." Autoscribe's positions, either in its infringement contentions or its Patent Owner's Preliminary Response in the IPR of the '621 Patent, demonstrate that its interpretation of these terms is not consistent with M&A's understanding of the terms' plain and ordinary meaning. Autoscribe should not be allowed to hide behind "plain and ordinary meaning" to advance theories that contradict the words of its patent. For the foregoing reasons, M&A Ventures respectfully requests that the Court adopt its proposed constructions

¹ Attached as Ex. B and referred to as "Shamos Decl." throughout.

of the disputed claim terms.

II. BACKGROUND OF THE '621 PATENT

The '621 Patent describes systems and methods for securely processing credit card transactions by limiting the credit card data that the merchant needs to store. The '621 Patent explains that because “[f]raud in credit card and other financial transactions is a major problem,” merchants who handle credit card data must expend significant resources to secure that credit card data. Ex. A, '621 Patent, 1:24-25; 1:45-48. Merchants can reduce these costs by hiring credit card processing organizations who use a technique called *tokenization* to limit the merchant’s access to (and therefore responsibility for securing) credit card data. '621 Patent, 1:49-52.

Tokenization replaces credit card data like a credit card number or expiration date with a *token*, a “symbolic representation” of the credit card data. '621 Patent, 1:52-59. Because the token is only meaningful to the transaction’s participants, the token is not subject to the same heightened security as credit card data. '621 Patent, 1:63-2:3. Therefore, tokenization may reduce a merchant’s costs. Tokenization was well known before the '621 Patent. '621 Patent, 1:49-52. The '621 Patent claims a form of tokenization in which a transaction is processed without the *merchant server* transmitting, processing or storing financial account data, thereby “reduc[ing] the potential liability of the merchants for data loss. . .” '621 Patent, 5:62-6:2. Instead, a separate *secure server* receives and stores the *payer*’s (i.e. customer’s) financial

account information.

Autoscribe asserts all 27 claims of the '621 Patent. The '621 Patent includes five independent claims. Claims 15 and 23 recite the required tokenization steps from the merchant server's perspective; claims 1, 8, and 25 recite the steps from the secure server's perspective.

III. LEGAL STANDARD

The intrinsic record—which consists of the claims themselves, the patent specification, and the prosecution history—is the best source for understanding the meaning of the claims. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1317 (Fed. Cir. 2005). Courts may also consider extrinsic evidence, such as technical dictionaries, treatises, and expert testimony, when construing claims. *Id.*

Patent claims must particularly point out and distinctly claim the subject matter regarded as the invention. 35 U.S.C. § 112(b). A claim, when viewed in light of the intrinsic evidence, must “inform those skilled in the art about the scope of the invention with reasonable certainty.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 910 (2014). If it does not, the claim fails § 112(b) and is therefore invalid as indefinite. *Id.* It is not enough that “a court can ascribe some meaning to a patent’s claims.” *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1370–71 (Fed. Cir. 2014) (quoting *Nautilus*, 572 U.S. at 911). Instead, “[t]he claims, ... must provide objective boundaries for those of skill in the art.” *Id.* at 1371. Indefiniteness, like

claim construction, should be assessed from the viewpoint of a person of ordinary skill in the art (“POSITA”) at the time the patent was filed. *Nautilus, Inc.*, 572 U.S. at 909. Indefiniteness is a question of law that the Court can resolve. *Teva Pharms. USA, Inc. v. Sandoz, Inc.*, 574 U.S. 318, 321 (2015).

Here, Dr. Shamos’s testimony is the only evidence in the record of how a POSITA would understand the ’621 Patent.

IV. ARGUMENT

A. “perform[ing] each software process required to maintain compliance with one or more information security standards”

Claim Term (1, 8, 25)	Autoscribe’s Proposal	M&A’s Proposal
“perform[ing] each software process required to maintain compliance with one or more information security standards”	Plain and ordinary meaning	Indefinite

Claims 1, 8, and 25 require the claimed secure server to store the payer’s sensitive financial account information in a secure storage location (i.e., the secure server) and then perform “each software process required to maintain compliance with one or more *information security standards*.” The intrinsic record does not clearly define “information security standards” and that phrase was not a term of art in 2012, the earliest priority date to which the ’621 Patent could be entitled. Shamos Decl., ¶¶ 50, 60-64. A POSITA would not have understood whether a specific source of guidance was a claimed “information security standard” and therefore Claims 1,

8, and 25 do not distinctly claim the subject matter of the invention and are indefinite.

The '621 Patent does not provide a specific definition of the phrase “information security standard.” Shamos Decl., ¶ 50. In fact, the '621 Patent's specification only uses the phrase “information security standard” once, in reference to the Payment Card Industry Data Security Standard (“PCI DSS”): “The Payment Card Industry Data Security Standard (PCI DSS) is an *information security standard* for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.” '621 Patent, 1:30-33 (emphasis added). Based on this disclosure, a POSITA would have understood that PCI DSS was a claimed “information security standard.” Shamos Decl., ¶ 57.

Autoscribe could have limited its claims to software processes required by PCI DSS. In response to office actions, Autoscribe attached PCI DSS v. 2.0 twice (Ex. C at ASC000194, ASC000314) and listed seven steps required for complying with PCI DSS (Shamos Decl., ¶ 56). But Autoscribe did not limit the claims to compliance with PCI DSS—and notably, Autoscribe does not argue the claims are so limited here—instead broadening its claims to capture nebulous “information security standards” without helping a POSITA determine whether guidance is or is not an “information security standard.” The claims are not even limited to standards relating to safeguarding financial account information, and a POSITA would have understood the broad “information security standards” to encompass cybersecurity

more generally. Shamos Decl., ¶ 58.

Autoscribe further confused the issue by referring throughout the specification to “industry standards,” “acknowledged security standards,”² and “best practices.” Shamos Decl., ¶ 58. And a POSITA would have known of state and federal legislation, regulations, and other industry-driven efforts relating to cardholder data and consumer privacy. *Id.* at ¶¶ 61-64.

Dr. Shamos’s un rebutted testimony shows a POSITA would not have understood how to determine whether a given protocol was an information security standard. *Id.* at ¶ 64. The fact that a POSITA would have known PCI DSS was within the claim scope does not save the claims. It is not enough that “a court can ascribe some meaning to a patent’s claims.” *Interval Licensing*, 766 F.3d at 1370–71 (quoting *Nautilus*, 572 U.S. at 911). To withstand definiteness review, a claim must contain objective boundaries to provide a POSITA sufficient notice to understand the invention. *Id.*; *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1364 (Fed. Cir. 2018). A single example in the specification is insufficient to provide a sufficiently definite boundary. *See Interval Licensing*, 766 F.3d at 1373–74 (citing *Enzo Biochem, Inc. v. Applera Corp.*, 599 F.3d 1325, 1336 (Fed. Cir. 2010)).

² This portion of the specification merely refers again to PCI, stating that the claimed secure server “preferably meets acknowledged security standards, such as PCI compliance.” ’621 Patent, 10:51-57.

B. “sensitive financial account information”

Claim Term (1, 8, 25)	Autoscribe’s Proposal	M&A’s Proposal
“sensitive financial account information”	Plain and ordinary meaning	Indefinite; alternatively, “financial account information whose storage requires compliance with one or more information security standards”

A POSITA would understand that the ’621 Patent distinguishes between information whose storage requires heightened security measures like those required by PCI DSS and information whose storage does not. Shamos Decl., ¶ 66. The benefit of the claimed invention is that it allows the merchant server to outsource the processing of cardholder data to the secure server, avoid storing information that requires heightened security measures, and therefore reduce the merchant server’s compliance costs. Ex. C at ASC000207; ’621 Patent, 1:45-48.

By contrast, the token is “non-sensitive data” which can be stored without requiring PCI compliance and is therefore provided to the merchant server. ’621 Patent, 1:63-2:3. “In a preferred embodiment, financial account information used to make one or more payments is submitted to the secure server while other less sensitive data elements such as customer’s name and address are submitted to the merchant’s regular server.” ’621 Patent, 2:35-39; *see also* 8:8-14.

The claims also make this distinction. On the one hand, “*sensitive* financial account information” must be stored in a “secure storage location” and transactions

should be processed “without providing the sensitive financial account information to the merchant server.” ’621 Patent, Claims 1, 8, 25. On the other hand, the *non-sensitive* token is provided to the merchant server. *Id.*

With this context, a POSITA would recognize that, as claimed, the sensitive financial account information is information whose storage requires compliance with information security standards. However, as discussed above, a POSITA would not understand how to determine whether a given set of guidance is an “information security standard.” Therefore, a POSITA would also not have understood with reasonable certainty the boundaries of what would qualify as “sensitive” information. Shamos Decl., ¶ 70.

If the Court does not find that the term “sensitive financial account information” is indefinite, it should be construed as “financial account information whose storage requires compliance with one or more information security standards.”

C. “obtainin[ing]” and “forward[ing]” a payment amount

Claim Term (1, 2, 8, 9, 15, 23, 25)	Autoscribe’s Proposal	M&A’s Proposal
“obtain[ing] the [second] payment amount		“obtain[ing] the money required for the [second] payment”

forward[ing] at least a portion of the [second] payment amount”	“obtaining the payment amount and causing or requesting at least a portion of the payment amount to be sent, directed, or credited”	“forward[ing] at least a portion of the money required for the [second] payment”
---	---	--

All independent claims of the ’621 Patent require obtain[ing] the payment amount and forward[ing] the payment amount. M&A’s construction properly addresses the two issues present for the Court: (1) clarifies that the “payment amount” refers to money, not just information about how much money should be paid, and (2) requires that the secure server forward that money. The Court should adopt M&A’s construction for these terms as it is consistent with the claim language, specification, and prosecution history.

1. “Payment amount” refers to money paid to the merchant, not just information about the payment.

M&A’s proposed construction clarifies that “payment amount” should be understood as “the money required for payment.” Autoscribe has not disputed this point to date in the parties’ conferences regarding claim construction. Clarification of “payment amount” is required because the claims use that term inconsistently. One of the first steps in the method of Claim 1 requires the secure server’s software to receive, from the merchant server, “at least one data element associated with the payer and a payment amount from the payer to the payee.” *See also*, ’621 Patent, Claims 8 and 23. Claims 15 and 23 similarly recite that the merchant server provides

the secure server with the data element and “a payment amount from the payer to the payee.” Here, the payer is the customer and the payee is the merchant. In these steps, the merchant is not providing the secure server with money; the merchant is instead informing the secure server about the transaction value. In context, payment amount here means information, not money. As used later in the claims however, including in the obtaining and forwarding limitations, the phrase “payment amount” means money, not merely information.

These claim terms are best understood within the context of the broader claim limitation. The entire limitation of Claims 1, 8, and 25 which includes the terms recites:

[P]rocessing the payment transaction using the sensitive financial account information by generating and transmitting an electronic request requesting the payment amount from the financial account, obtaining the payment amount, and forwarding at least a portion of the payment amount to the payee.

Simply put, there are three steps articulated for processing the payment transaction:

- 1) generating and transmitting an electronic request requesting the payment amount;
- 2) obtaining the payment amount; and 3) forwarding at least a portion of the payment amount.

Autoscribe articulated these distinct steps during prosecution. In arguments against rejection under § 101, Autoscribe stated that the secure server provides API functions to the merchant server that:

- process the payment by
 - generating and transmitting an electronic request requesting the payment amount;
 - obtaining the payment amount; and
 - forwarding at least a portion of the payment amount.

Ex. C at ASC000664.

To “process” the payment transaction, money must move from the customer’s account to the merchant’s account. *See* ’621 Patent, 9:16-19 (“The operator of the secure server 202 then processes the payment using the financial account pointed to by the token, and makes the proceeds available to the merchant.”). Further, the “obtaining” step would be redundant if it merely required the secure server to obtain information about the transaction value as the merchant server provides the transaction value to the secure server in a differently recited limitation. Claim terms should be interpreted so as not to make claim language superfluous. *Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.*, 853 F.3d 1272, 1288 n.10 (Fed. Cir. 2017) (“It is highly disfavored to construe terms in a way that renders them void, meaningless, or superfluous.”).

2. The secure server must “forward” at least a portion of the payment, not merely cause another to do so.

Further, Autoscribe told the Examiner that each of these three steps (generating, obtaining, and forwarding) are performed *by the secure server*. Ex. C at ASC000664. Autoscribe’s characterization is consistent with the claim language. Claims 15 and 23 recite “generating a payment transaction instruction... that... *instructs the secure server to...* obtain the payment amount and forward at least a

portion of the payment amount.” ’621 Patent, Claims 15 and 23 (emphasis added). This language is instructive as to the meaning of the terms across all claims as “[t]he claims themselves provide substantial guidance as to the meaning of particular claim terms.” *Phillips*, 415 F.3d at 1314 (Fed. Cir. 2005). The specification also supports that processing the payment is performed by the secure server. *See* ’621 Patent 10:54 (“The secure server 202 processes transactions...”).

Autoscribe impermissibly attempts to broaden the scope of the claim beyond what is disclosed in the specification as it attempts to sweep in performance of the steps of processing the payment action by something other than the secure server. In particular, Autoscribe seeks to construe “forwarding at least a portion of the payment amount” as “causing or requesting at least a portion of the payment amount to be sent, directed, or credited.” Such a construction would encompass performance of the payment transaction step by something other than the secure server. There is nothing in the claim language, specification, or prosecution history to support this construction. The claims must be construed faithfully to the invention disclosed in the specification. *See Wi-Fi One, LLC v. Broadcom Corp.*, 887 F.3d 1329, 1346 (Fed. Cir. 2018). Further, Autoscribe’s construction seeks only to broaden the scope of one step of the three-step payment process. There is nothing in the specification or prosecution history that indicates that the forwarding element should be treated or understood differently than the generating or obtaining steps.

D. “authenticate[s] a payee” / “authenticating the payee”

Claim Term (1, 8, 15, 23, 25)	Autoscribe’s Proposal	M&A’s Proposal
“authenticate[s] a payee”/ “authenticating the payee”	Plain and ordinary meaning	“verify[ies] the identity of the payee/verifying the identity of the payee”

The Court should construe the terms “authenticate[s] a payee”/ “authenticating the payee” as “verify[ies] the identity of the payee/verifying the identity of the payee” because this construction is both consistent with the specification and supported by extrinsic evidence of how a POSITA would understand the term in the field of the patent.

The specification does not specifically recite the process for authenticating a “payee.” However, the specification provides ample support for authenticating a customer (payer), and these disclosures shed light on how Autoscribe used the word “authenticating.” *See* ’621 Patent, 10:15-19 (“the customer may be invited to enter a shared secret, such as an assigned access key, partial or complete social security number, account number, telephone number, password, or other data to authenticate the customer”); 2:25 (“customer (also sometimes referred to as the payer)”). Specifically, the authenticated payer enrollment session is completed via a communications link such as a telephone or internet link to “verify the identity of the user.” *See* ’621 Patent 2:19-22; 12:54-58; 13:7. “Authentication” should be similarly understood as requiring verification of the identity of the payee in claims

which require authenticating the *payee*. Where “a patent repeatedly and consistently characterizes a claim term in a particular way, it is proper to construe the claim term in accordance with that characterization.” *Wisconsin Alumni Rsch. Found. v. Apple Inc.*, 905 F.3d 1341, 1351 (Fed. Cir. 2018).

M&A’s proposed construction is consistent with dictionary definitions for the term “authentication.” Ex. H, Wiley Electrical and Electronics Engineering Dictionary (2004) at 298 (“Authentication. In computers and communications, the process of verifying the legitimacy of a transmission, user, or system. Measures such as passwords and digital signatures are employed.”); Ex. I, Dictionary of Computer Science (2016) at 32 (“Authentication. A process by which subjects, normally users, establish their identity to a system. This may be effected by the use of a password or possession of a physical device, e.g., a coded token.”).

M&A’s proposed construction is consistent with the plain and ordinary meaning of the term. Autoscribe proposes that the claim need not be construed beyond plain and ordinary meaning. However, Autoscribe’s interpretation of the claim term as expressed in its Infringement Contentions indicates that there is a disagreement regarding the plain and ordinary meaning of the term. Autoscribe’s Infringement Contentions allege the Accused Product “provides an API that performs a method of authenticating (e.g., authorizing, verifying, confirming, etc.) the payee” and cites to M&A’s product as “showing a method of authorization using

apptoken.” Ex. G, Autoscribe’s Infringement Contentions Exhibit A at 13. “Authenticate” does not mean “authorize” and M&A’s construction clarifies that authorization is not within the claim scope.

Autoscribe’s interpretation is inconsistent with use of term “authorize” throughout the patent. The ’621 Patent does not use the term “authorize” as “verifying the identity of the customer.” *See* ’621 Patent, 2:64-3:3 (“The token is ...used to identify the customer account to be debited to process a payment authorized by the customer.”); 3:9-15 (discussing “authorized” payments). In other words, authenticating focuses on verifying a user’s identity; authorizing focuses on whether certain actions are allowed or permitted.

The terms “authenticate” and “authorize” should have separate meanings as “the general assumption is that different terms have different meanings” and there is nothing in the specification to indicate otherwise. *PPC Broadband, Inc. v. Corning Optical Commc’ns. RF, LLC*, 815 F.3d 747, 752–753 (Fed. Cir. 2016) quoting *Symantec Corp. v. Comput. Assocs. Int’l, Inc.*, 522 F.3d 1279, 1289 (Fed. Cir. 2008). The parties disagree on the plain and ordinary meaning of the claim term. The Court should resolve any dispute regarding the scope of the asserted claims prior to the issue being presented before the jury. *See O2 Micro Int’l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 13601-61 (Fed. Cir. 2008).

E. “function”

Claim Term (1, 8, 15, 23, 25)	Autoscribe’s Proposal	M&A’s Proposal
“function”	Plain and ordinary meaning	“block of code that operates as a single logical unit”

The claim term “function” should be construed as “a block of code that operates a single logical unit.” The term “function” has a distinct meaning in the context of software development and computer engineering. A function within a computer program is defined as “a small group of instructions which perform a given task. Also called a subroutine (2), routine (1), or procedure (2).” Ex. H, Wiley Electrical and Electronics Engineering Dictionary (2004) at 306. A function can also be understood as “[a] piece of code that operates a single logical unit.” Ex. J, Dictionary of Computer and Internet Terms Vol. 1 (2016) at 217. These dictionary definitions provide the Court with the initial context under which the claim term should be understood. *See Phillips*, 415 F.3d at 1324 (“[A] judge who encounters a claim term while reading a patent might consult a general purpose or specialized dictionary to begin to understand the meaning of the term, before reviewing the remainder of the patent to determine how the patentee has used the term.”).

The specification and claims use the term “function” consistently with the above included dictionary definitions and the use of the term “function” in computer programming. For example, the specification articulates example embodiments

having functional subroutines performing steps of the payment process which at their conclusion advance to the next function in the calling program. *See* '621 Patent, 13:55-57, 14:60-62. Therefore, the term “function” would be understood within its proper context as a “block of code that operates as a single logical unit.” M&A’s proposed construction of the term is consistent with the plain and ordinary meaning.

Autoscribe proposes that the term need no construction beyond its plain and ordinary meaning. However, it is clear from Autoscribe’s Infringement Contentions that the plain and ordinary meaning of the term is in dispute. For example, Autoscribe’s Infringement Contentions recite numerous, disparate portions of M&A source code as satisfying the financial account registration function. Ex. G, Autoscribe Infringement Contentions Exhibit A at 14-33. M&A would contend that all steps of the financial account registration function (as well as any other recited function) must be included within a block of code that operates as a single logical unit. Under the plain and ordinary meaning of the term “function,” Autoscribe cannot recite to unconnected portions of source code across multiple products as satisfying the claim term requiring a “function.” As with the immediately above term, construction of this claim term is necessary where the parties are clearly in dispute. *See O2 Micro*, 521 F.3d at 1360-61.

F. “providing a non-sensitive data token to the merchant...without providing the non-sensitive data token to the payer”

Claim Term (1, 8, 25)	Autoscribe's Proposal	M&A's Proposal
“providing a nonsensitive data token to the merchant... without providing the non-sensitive data token to the payer”	Plain and ordinary meaning	“during the token retrieval function, provide a non-sensitive data token to the merchant without providing the non-sensitive data token to the payer”

The limitation included in Claims 1, 8, and 25 reciting “providing a nonsensitive data token to the merchant... without providing the non-sensitive data token to the payer” should be construed as “during the execution of the token retrieval function, providing a non-sensitive electronic data token representing the sensitive financial account information to the merchant... without providing the non-sensitive electronic data token to the payer.” In short, the claim language requires only that, during the token retrieval function, the secure server does not provide the token to the payer when it provides the token to the merchant. The claim language should not be understood as requiring that the server must never provide the token to the payer. Construction of this claim term is necessary to resolve any confusion for the jury regarding the scope of the claims. *See Eon Corp. IP Holdings v. Silver Spring Networks*, 815 F.3d 1314, 1319 (Fed. Cir. 2016); *see also Every Penny Counts, Inc. v. Am. Express Co.*, 563 F.3d 1378, 1383 (Fed. Cir. 2009) (“[T]he court’s obligation is to ensure that questions of the scope of the patent claims are not

left to the jury. In order to fulfill this obligation, the court must see to it that disputes concerning the scope of the patent claims are fully resolved.” (citation omitted)).

Claims 1, 8, and 25 each include two discrete functions: (1) the financial account registration function and (2) the token retrieval function. These claims recite that the API “executes the financial account registration function, upon initiation by the merchant server by” and then includes recitation of several steps for executing the financial registration function. ’621 Patent, Claims 1, 8, and 25. The claims then separately recite “executing a token retrieval function, upon initiation by the merchant server via the API” and then further includes the step of “providing a non-sensitive electronic data token ... to the merchant ... without providing the non-sensitive electronic data token to the payer...” *Id.* Thus, the claims specifically delineate providing the token “without providing the non-sensitive electronic data token to the payer” is performed during execution of the token retrieval function.

The prosecution history of the ’621 Patent supports this understanding. To overcome § 101 rejections, Autoscribe amended the claims to recite separate financial account registration and token retrieval functions. These amendments grouped certain steps as being part of one of the functions. *See* Ex. C at ASC000582 (notes made in claim amendment that certain steps are included as “part of the financial registration function” and separately recites certain steps executed “upon the initiation of the token retrieval function”).

Thus, Autoscribe made clear that the limitations recited under the token retrieval function, including “providing a non-sensitive electronic data token to the merchant... without providing the non-sensitive electronic data token to the payer,” are separate from the financial account registration function. *See Schindler Elevator Corp. v. Otis Elevator Co.*, 593 F.3d 1275, 1285 (Fed. Cir. 2010) (“[A]n amendment that clearly narrows the scope of a claim, such as by the addition of a new claim limitation, constitutes a disclaimer of any claim interpretation that would effectively eliminate the limitation or that would otherwise recapture the claim’s original scope.”). Thus, the limitations recited with respect to the token retrieval function define what does and does not happen during the execution of the token retrieval function.

The specification also supports this understanding. The specification distinguishes the financial account registration and token retrieval functions, stating that “[a] hosted system on a secure server 202 provides Financial Account Registration functions and Token Retrieval functions.” ’621 Patent, 5:58-62; *see also* 6:63-7:1, 7:1-8. The specification describes the secure server sending the token to the merchant server during the token retrieval functions but does not describe sending the token during any other step in the payment process. *See e.g.*, ’621 Patent, 7:31-34 (“Secure server 202 ... stores the financial account information received from the customer... and provides a token to merchant server 204.”). The

specification never explicitly states that the token cannot be sent to the payer during any other step of the payment process. In fact, the '621 Patent states that the token is “only meaningful to the merchant,” implying that it is not meaningful to the payer. '621 Patent, 10:46-48. Thus, the '621 Patent does not give a reason to prevent the token from being sent to the payer.

Additionally, the '482 application, incorporated by reference in the '621 Patent, contemplates that the non-sensitive electronic data token is provided to the payer outside of execution of the token retrieval function. The '482 application explains that “[t]he hosted system [secure server] returns a token or other account identifier to the user [payer] and/or the merchant’s system when the financial account information has been registered at the hosted system.” Ex. D, '482 Application at 21. Thus, the '482 application discloses that the token may be sent to the payer at other times such as during the financial account registration function.

Therefore, in view of the structure of the claim, the specification, and the prosecution history the Court should construe this limitation as “*during the token retrieval function*, providing a non-sensitive data token to the merchant without providing the non-sensitive data token to the payer” to provide the jury with an understanding as to the scope of the claims.

G. “receiving the non-sensitive electronic data token from the secure server, wherein...the secure server does not provide the non-sensitive electronic data token to the payer”

Claim Term (15, 23)	Autoscribe's Proposal	M&A's Proposal
“receiving the non-sensitive electronic data token from the secure server, wherein...the secure server does not provide the non- sensitive electronic data token to the payer”	Plain and ordinary meaning	“during the token retrieval function, receiving a non-sensitive data token without the secure server providing the non-sensitive data token to the payer”

The claim term “receiving the non-sensitive electronic data token from the secure server, wherein... the secure server does not provide the non-sensitive electronic data token to the payer” recited in Claims 15 and 23 should similarly be understood as “*during the token retrieval* function, receiving a non-sensitive data token without the secure server providing the non-sensitive data token to the payer.” ’621 Patent, Claims 15 and 23. As with the other independent claims, Claims 15 and 23 recite the payment process in two discrete functions (1) the financial account registration function and (2) the token retrieval function. The claim limitation “the secure server does not provide the non-sensitive electronic data token to the payer” applies to the token retrieval function.

During the financial account registration function, Claims 15 and 23 recite that the encrypted financial account information is transmitted to the secure server “without providing the sensitive financial account information to the merchant server.” Similarly, during the “token retrieval function,” the claims also recite the merchant server receives the non-sensitive electronic data token “wherein the

merchant server does not receive the sensitive account information.” *Id.* Therefore, the claims specify that the financial account information is not sent to the merchant server both during the financial account registration function and during the token retrieval function. In contrast, the claims only require “the secure server does not provide the non-sensitive electronic data token to the payer” during the token retrieval function and is otherwise silent as to the financial account registration function.

During prosecution, Autoscribe also amended Claim 15 (pending as claim 31) and Claim 23 (pending as claim 46) to recite the separate financial account registration and token retrieval functions and grouped certain steps as being part of one of the two functions. *See* Ex. C at ASC000572, 575. By making these amendments to recite the functions separately, Autoscribe made clear that the limitations under the token retrieval function, like “the secure server does not provide the non-sensitive electronic data token to the payer” are separate from the limitations under the financial account registration function. *See Schindler Elevator*, 593 F.3d at 1285. The specification supports this construction for the same reasons articulated in Section F above. As also articulated above, Autoscribe’s interpretation of whether the secure server ever provides the token to the payer under the Autoscribe’s plain and ordinary meaning of the term differs from M&A’s understanding of the plain and ordinary meaning.

This claim term should be similarly construed to provide guidance to the jury regarding the scope of the claims. Claims 15 and 23 should be understood as requiring the secure server to not provide the token to the payer only during the token retrieval function and that the token may otherwise be sent to the payer during another step in the payment process.

H. “generating a uniform resource locator (url),... the url comprising either: a dynamic url generated by the secure server...; or a static url and a hypertext transport protocol (http) parameter...”

Claim Term (1, 8, 25)	Autoscribe’s Proposal	M&A’s Proposal
“generating a uniform resource locator (url),... the url comprising either: a dynamic url generated by the secure server...; or a static url and a hypertext transport protocol (http) parameter...”	Plain and ordinary meaning	“providing a URL that is either: (1) a dynamic URL generated by secure server or (2) a static URL known to the merchant and a parameter”

The exact claim language of Claims 1, 8, and 25 recites:

generating a uniform resource locator (URL), for establishing a secure socket layer connection via the internet between the secure server and the payer computing system, the URL comprising either:
a dynamic URL generated by the secure server for the payer and the payee; or
a static URL and a hypertext transport protocol (HTTP) parameter used by the secure server to identify the payer and the payee

The generating step should be construed such that “generating” the URL statically includes the secure server “generating” the URL by prompting the

merchant server to combine a predefined static URL with an “HTTP parameter.” In other words, “generating a uniform resource location” is not strictly limited to require that the URL be generated entirely at the secure server.

The claim language itself informs this construction. The claim recites that “generating a URL” includes either: (1) “a dynamic URL generated by the secure server” or (2) “a static URL” known to the merchant and a “hypertext transport protocol (HTTP) parameter used by the secure server to identify the payer and payee.” For (1) the dynamic URL, the claims explicitly recite that the dynamic URL be generated by the secure server. Conversely, for (2) the static URL the claim does not recite that a static URL be generated “by the secure server.”

The specification also distinguishes between the dynamic method (in which the URL is generated by the secure server) and the static method (in which the URL is generated by prompting the merchant server to combine a static URL with the HTTP parameter). During the dynamic method, the secure server executes subroutine 3. ’621 Patent, 11:60-62. Subroutine 3 provides “a financial account registration entry form.” *Id.* “In step 430 [of subroutine 3], the API [of the secure server] creates a registration URL.” *Id.* at 14:46-47. Thus, the “registration URL” or dynamic URL is generated in subroutine 3.

In contrast, when the static URL method is used, subroutine 3 is not performed and the secure server does not generate a new URL. *Id.* at Fig. 4d. Thus, step 430 of

subroutine 3 in which the secure server generates the registration URL is not performed. Instead, an SSL connection is established using a static URL combined with an array of codes: “The payment application then displays an array of codes in step 548 and launches a web browser with a financial account registration URL [in step] 550.” *Id.* at 12:58-60. The static URL method never describes the secure server generating a new financial account registration URL.

Additionally, the ’482 application similarly distinguishes how the dynamic and static URLs are generated. The ’482 application explains that, in the dynamic URL method, a “temporary URL” is request from the secure server. Ex. D, ’482 Application at 62. In the static URL method, however, a “temporary array of codes” is requested from the secure server and submitted on a Financial Account Registration site. *Id.* Thus, the static URL is not requested from and, thus, not generated anew by the secure server.

M&A’s proposed construction is consistent with the plain and ordinary meaning for the term and provides clarity to the jury regarding the grammatical structure of the claim. M&A proposed the construction of this term consistently in their IPR petition. Ex. E, IPR Petition at 17. In its preliminary response, Autoscribe disputed that the term needs construction and proposed that the term be given its plain and ordinary meaning as it has done so here. Ex. F, Patent Owner’s Preliminary Response, at 15. Autoscribe does not articulate why M&A’s proposed construction

is not consistent with the plain and ordinary meaning of the term. However, Autoscribe maintains a dispute with M&A’s construction, and thus, the Court should construe this claim.

I. The “representation of the non-sensitive electronic data token” terms

Claim Term (2, 9, 15, 23)	Autoscribe’s Proposal	M&A’s Proposal
“a representation of the non-sensitive electronic data token”	Plain and ordinary meaning	Indefinite
Claim Term (3, 10, 16)	Autoscribe’s Proposal	M&A’s Proposal
“wherein the representation of the non-sensitive electronic data token is the nonsensitive electronic data token”	Plain and ordinary meaning	Indefinite

Claims 2, 9, 15, and 23 all require that the merchant server send to the secure server a transaction payment instruction that includes “a representation of the non-sensitive electronic data token.” Dependent claims 3, 10, and 16 further require that “the representation of the non-sensitive electronic data token is the nonsensitive electronic data token.” A POSITA would recognize that the available evidence about this limitation falls into two, mutually exclusive categories.

On one hand, the ’621 Patent’s use of the word “representation” demonstrates that the representation must be *different from* the thing it represents. In other words, the representation of the token must differ from the token itself. On the other hand, dependent claims 3, 10, and 16 require that the representation of the token is the

token. Where the intrinsic record is inconsistent about the meaning of a claim term, and therefore there is no clear construction available, the claim is indefinite. *HZNP Medicines LLC v. Actavis Labs. UT, Inc.*, 940 F.3d 680, 698 (Fed. Cir. 2019). Here, a POSITA would not understand how to reconcile the contradictory evidence, and Claims 2, 3, 9, 10, 15, 16, and 23 do not inform a POSITA with reasonable certainty about the scope of the invention and are indefinite.

**1. Intrinsic and extrinsic evidence indicates that a
“representation” differs from the thing it represents.**

Significant intrinsic and extrinsic evidence indicates that the “representation of the token” as recited in Claims 2, 9, 15, 23 would be different than the token itself.

The standard English meaning of “representation” is something that shows, describes, or represents something *else*. Exhibit K, American Heritage Dictionary (2018) at 1490; Exhibit L, Longman Dictionary of American History (2014) at 947. The ’621 Patent almost always uses the term “representation” consistent with that meaning. The ’621 Patent explains that a token, as used in the context of electronic payment processing, is a “symbolic *representation*” of credit card data. ’621 Patent, 1:52-59; 10:46-48. The specification makes clear that the token is not the credit card data itself.

First, the token and the credit card data have different properties. While the credit card data is “sensitive data” that must be securely stored and transmitted, the token is “not considered sensitive outside the environment where it is stored and

used.” ’621 Patent, 1:52-55. Second, a merchant may possess the token without possessing the corresponding financial account information. *See id.* 3:9-15 (explaining that with the token, the merchant can process payments whenever authorized “but does not hold the underlying financial account information. . .”); 8:40-43 (“The token is a pointer that allows the payee to reference the financial account information of that payer without possessing the actual financial account information.”); Shamos Decl., ¶¶ 75-77.

The claims also support the conclusion that the representation of the token is different than the token itself. Claim 2 separately recites “a representation of the non-sensitive electronic data token” and “the non-sensitive electronic data token.” Generally, where claim elements are listed separately, “‘the clear implication of the claim language’ is that those elements are ‘distinct component[s]’ of the patented invention.” *Becton, Dickinson and Co. v. Tyco Healthcare Group, LP*, 616 F.3d 1249, 1254 (Fed. Cir. 2010) (citing *Gaus v. Conair Corp.*, 363 F.3d 1284, 1288 (Fed. Cir. 2004) and *Engel Indus., Inc. v. Lockformer Co.*, 96 F.3d 1398, 1404–05 (Fed. Cir. 1996)). Applying this canon of claim construction, a POSITA would understand from the evidence discussed in this section that a “representation of the token” as recited in Claims 2, 9, 15, 23 would be different than the token itself.

**2. Different intrinsic evidence demonstrates that a
“representation of the token” includes the token.**

Other intrinsic evidence, however, indicates the exact opposite: that the

representation of the token can include the token. Claims 3, 10, and 16 all recite “wherein the representation of the non-sensitive electronic data token is the non-sensitive electronic data token.” And the only portion of the specification that discusses the “representation of the token” later conflates that representation with the token itself:

Next, in step 314, at any time after registration is complete, the payee can process an authorized payment from the payer by electronically generating a payment transaction instruction in the first computing system, including a *representation of the token*, and electronically transmitting the payment transaction instruction to a computing system other than the first computing system having access to said financial account information. For example, the instruction may be transmitted to the second computing system, e.g., the secure server 202. ... The second computer system or another computer system that receives the instructions and *token* (and can access the financial account information based on the token) processes the payment as requested, without the first computing system having any direct access to the payer's financial account information represented by the token.

’621 Patent, 8:52-9:11 (emphasis added). In other words, the specification describes that the first computing system, which is later claimed as the merchant server, generates “a payment transaction instruction” including “a representation of the token” and sends that instruction (presumably, with the “representation of the token” included) to the secure server. The secure server then receives the instructions and “token”—not the “representation of the token.” Notably, Autoscribe cited the quoted paragraph above (’621 Patent, 8:52-9:11) to the Examiner as support for the subject matter claimed in Claim 3, which recites that the representation of the token

is the token. Ex. C at ASC000120.

3. Any attempt to reconcile the evidence yields a nonsensical claim construction.

The entirety of the available intrinsic evidence from the '621 Patent specification, claims, and file history, and extrinsic evidence about the meaning of the word “representation” is inconsistent. The Federal Circuit confronted a similar circumstance in *HZNP Medicines LLC v. Actavis Labs. UT, Inc.*, 940 F.3d 680, 698 (Fed. Cir. 2019) when attempting to construe claims directed to a topical drug formulation with “better drying time” than prior art formulations. The specification stated that the inventive gel formulation demonstrated *more rapid* drying than the prior art liquid formulations. *Id.* at 698. However, the in vivo and in vitro test data reported in the specification demonstrated that the inventive gel formulations dried *more slowly* than prior art liquid formulations. *Id.* This inconsistency rendered the claims indefinite. *Id.* at 698-699. The same result is appropriate here.

Further, if a POSITA attempted to reconcile this available evidence, the result would be a construction that is nonsensical: i.e., that the representation of the token must differ from the token but can also be the token. Such a nonsensical construction would render the claims indefinite as well. *See Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357 (Fed. Cir. 1999) (declining to rewrite the claims “whereas here, claims are susceptible to only one reasonable interpretation and that interpretation results in a nonsensical construction of the claim as a whole, the claim

must be invalidated”).

Further, a POSITA would not understand how to differentiate between a token and the representation of the token as those terms are used in the claims. Shamos Decl., ¶ 78. Because a POSITA would not reasonably understand the claim scope, Claims 2, 3, 9, 10, 15, 16, and 23 are indefinite.

V. CONCLUSION

As demonstrated above, construction of the disputed terms is necessary to clarify the proper meaning of the claims and resolve the parties’ disputes regarding their scope. M&A Ventures’ proposed constructions resolve these issues while staying true to the claim language and the Patentee’s description of the claimed invention. Autoscribe should not be allowed to hide behind a plain and ordinary meaning to advance theories that directly contradict the words of the patent. For the foregoing reasons, M&A Ventures respectfully requests that the Court adopt its proposed constructions of the disputed claim terms.

Dated: December 12, 2024

/s/ Stephanie N. Sivinski

Richard Miller
Georgia Bar No. 065257
Ballard Spahr LLP
999 Peachtree Street NE, Suite 1600
Atlanta, Georgia 30062
Telephone: 678-420-9340
Email: millerrw@ballardspahr.com

David H. Harper (*pro hac vice*)
Texas Bar No. 09025540
david.harper@haynesboone.com
Stephanie N. Sivinski (*pro hac vice*)
Texas Bar No. 24075080
stephanie.sivinski@haynesboone.com
Marron E. Frith (*pro hac vice*)
TX Bar No. 24137884
marron.frith@haynesboone.com
Jamie Raju (*pro hac vice*)
TX Bar No. 24095717
jamie.jaju@haynesboone.com
HAYNES AND BOONE, LLP
2801 N. Harwood Street
Suite 2300
Dallas, Texas 75201
(214) 651-5000 (telephone)
(214) 200-0615 (fax)

**COUNSEL FOR DEFENDANT M&A
VENTURES, LLC**

CERTIFICATE OF SERVICE

I hereby certify that counsel of record was served this M&A Ventures LLC Opening Claim Construction Brief via the Court's ECF system on December 12, 2024.

/s/ Stephanie N. Sivinski

Stephanie N. Sivinski

CERTIFICATE OF COMPLIANCE

Pursuant to Local Rule 7.1(D), I hereby certify that the foregoing has been prepared in compliance with Local Rule 5.1(B) in 14-point Times New Roman font.

/s/ Stephanie N. Sivinski

Stephanie N. Sivinski